I would like to praise God for his unscathed donation of belief and empowerment upon myself not only in course of this work towards my Bachelor degree but throughout my entire life.
My deepest gratitude goes first and foremost to my supervisor **Dr. IBRAHIM KHIDER ELTAHIR**, for his constant support and guidance, patience during the whole period of this research.

Secondly I would like to express my greatest gratitude to my beloved teacher Rasha jalal for her guidance and to my beloved colleague Eng. Azza Kamal for her help during the implementation of the software.

Great appreciation goes to my Brother and my friend Ismail Najmuldin for his constant support.

To my friends and those who their name slipped and not mentioned thank you for your support and your encouragement.

I should mention that without my beloved family I would not even be where I am now. I am very blessed to have such family and thank them with all my heart for their prayer, encouragement and their time gave to me to do this study.

---

**مستندخص**

هذا البحث يتناول توضيح الطرق أمن المعلومات القديم منها والحديث حيث إنه يهدف إلى محافظة علي امن المعلومات النصيه (سريتها، خصوصيتها) وذلك بتسليطها
ABSTRACT

This dissertation is a description of the information security techniques and in the first place, it aimed to maintain the information security (privacy, Confidentiality) by encrypting it using RSA algorithm and hid it into image.
spatial domain using different algorithms like Least Significant Bit algorithm, Convolution or Bit XOR algorithm, Random approach algorithm, Least Significant Bit based Random approach algorithm, and Convolution based Random approach algorithm and hence transmits the image to the Receiver to Extract the information and decrypt it. Also it compares the effect of these algorithms on the image by calculating Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). And also it explains the relation between information Size and image size.

By using MATLAB language the Steganography system was implemented and it allow user to select an image and determine the Steganography algorithm and hence enter the information which it can be short message or file.

The results were obtained and discussed and it shows that the Random approach algorithms have visible impact on the image appears as black spot while Convolution algorithm or Least Significant Bit algorithm does not have a visible impact on the image because the precision in many image formats is far greater than that perceivable by average human vision. Also the results shows that the Least Significant Bit based Random approach algorithm and Convolution Based Random approach algorithm are the best because the information are embed randomly so no one except the receiver Know the order of the information in side
image and this add Another level of security to the information.
And it concludes that there are no visible impacts on the image when the PSNR is greater than 40dB and the information size is small compared to the image size.

Contents

Acknowledgment..............................................................................................................1

.. II
Chapter 1: Introduction
1.1 Preface ................................................................. 1
1.2 Problem Statement .......................................................... 3
1.3 Objectives ........................................................................ 4
1.4 Methodology .................................................................... 4
1.5 Thesis Outlines ................................................................. 5

Chapter 2: Security Background
Chapter 3: Security Techniques

3.1 Types of Cryptography algorithm

3.1.1 Public -Key Cryptography algorithm

3.1.1.1 RSA algorithm

3.2 Steganography Techniques

3.3 Image

3.3.1 Spatial domain

3.3.1.1 Least Significant Bit algorithm

3.3.1.2 Random Approach

3.3.1.3 Convolution or Bit XOR algorithm

3.3.1.4 Random approach based LSB algorithm

3.3.1.5 Random approach based Bit XOR algorithm

3.4 Algorithm Performance
3.4.1 Mean Square Error......................... .........................33
3.4.2 Peak Signal to Noise Ratio.. .........................34
3.4.3 Mean & Standard deviation.............. .........................34

Chapter 4: Simulation Tools and Result

4.1 Model Description ........................................36
   4.1.1 Transmitter Model ... 36
   4.1.2 Receiver Model .........................39

4.2 Simulation Software.........................................................41

4.3 Results and Discussions .........................41

4.4 Case Study .........................................................49
   4.4.1 Message Transmission..............................49
   4.4.2 File Transmission .........................................51

4.4.3 Help Dialog .........................................................54

Chapter 5: Conclusion and Recommendation

5.1 Conclusion .........................................................57
5.2
Recommendations .................................................................
...............58
References ...........................................................................
...59
Appendixes

List of Tables

<table>
<thead>
<tr>
<th>Tables Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2.1: Vigenere table</td>
<td>9</td>
</tr>
<tr>
<td>Table 2.2: The Playfair encipher tableau</td>
<td>13</td>
</tr>
<tr>
<td>Table 2.3: A simple test key system</td>
<td>16</td>
</tr>
</tbody>
</table>
## List of Figures

<table>
<thead>
<tr>
<th>Figure Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2.1: Monoalphabetic substitution cipher</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2.2: A vigenere polyalphabetic substitution cipher</td>
<td>8</td>
</tr>
</tbody>
</table>
Figure 2.3: A spy’s message
11
Figure 2.4: A spy’s claimed
11
Figure 2.5: Message manipulating
12
Figure 2.6: Playfair enciphering
13
Figure 3.1: Classification of the Steganography techniques
29
Figure 3.2: LSB insertion in 24 bit image
31
Figure 3.3: Convolution decoder machine
32
Figure 4.1: The preparing stage Flow chart 36
Figure 4.2: The preparing stage model 37
Figure 4.3: The second stage model 37
   Figure 4.4: The second stage flow chart 38
Figure 4.5: The Receiver model 39
   Figure 4.6: The Receiver flow chart 40
Figure 4.7: MSE of different sizes images by using LSB algorithm 41
Figure 4.8: PSNR of different sizes images by using LSB algorithm 42
Figure 4.9: MSE of different sizes images by using Convolution algorithm
Figure 4.10: PSNR of different sizes images by using Convolution algorithm
Figure 4.11: MSE of different sizes images by using Random approach algorithm
Figure 4.12: PSNR of different sizes images by using Random approach algorithm
Figure 4.13: The effect of Random approach algorithm On the kids image
Figure 4.14: The effect of Random approach algorithm On the football image
Figure 4.15: MSE of different sizes images by using LSB based Random approach algorithm
Figure 4.16: PSNR of different sizes images by using LSB based Random approach
Figure 4.17: MSE of different sizes images by using
Convolution based Random approach algorithm

Figure 4.18: PSNR of different sizes images by using 48
Convolution based Random approach algorithm

Figure 4.19: Insertion model for Short message 49
Figure 4.20: Image save operation 50
Figure 4.21: Successful of the image save operation 50
Figure 4.22: The Receiver model for Short message 51
Figure 4.23: File insertion model 52
Figure 4.24: Help operation model 52
Figure 4.25: Image save operation model 53
Figure 4.26: The successful of image save operation 53
Figure 4.27: The Receiver model for file 54
Figure 4.28: Insertion of large file 55
Figure 4.29: Appear a warning message 55
Figure 4.30 Insertion of large files 56
Figure 4.31: Appear a warning message 56
# List of Abréviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advance encryption standard</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard.</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>GIF</td>
<td>Graphics interchange file</td>
</tr>
<tr>
<td>LSB</td>
<td>Least Significant Bit</td>
</tr>
<tr>
<td>MATLAB</td>
<td>MATrix LABoratory</td>
</tr>
<tr>
<td>MSE</td>
<td>Mean Square Error</td>
</tr>
<tr>
<td>Pixel</td>
<td>Picture element</td>
</tr>
<tr>
<td>PKC</td>
<td>Public Key Cryptography.</td>
</tr>
<tr>
<td>PSNR</td>
<td>Peak Signal to Noise Ratio</td>
</tr>
<tr>
<td>RSA</td>
<td>Ronald Rivest Adi Shamir Leonard Adleman</td>
</tr>
<tr>
<td>SKC</td>
<td>Secret Key Cryptography.</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol /Internet Protocol</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
</tr>
</tbody>
</table>